AF
JFW

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/640,839
Filing Date	08/16/2000
First Named Inventor	Mark McClanahan
Art Unit	2132
Examiner Name	Benjamin E. Lanier
Attorney Docket Number	RPS920000052US1
Total Number of Pages in This Submission	45

ENCLOSURES (*Check all that apply*)

- ☑ Fee Transmittal Form
  - □ Fee Attached
- □ Amendment/Reply
  - □ After Final
  - □ Affidavits/declaration(s)
- □ Extension of Time Request
- □ Express Abandonment Request
- □ Information Disclosure Statement
- □ Certified Copy of Priority Document(s)
- □ Reply to Missing Parts/ Incomplete Application
  - □ Reply to Missing Parts under 37 CFR 1.52 or 1.53

- □ Drawing(s)
- □ Licensing-related Papers
- □ Petition
- □ Petition to Convert to a Provisional Application
- □ Power of Attorney, Revocation Change of Correspondence Address
- □ Terminal Disclaimer
- □ Request for Refund
- □ CD, Number of CD(s) ____________
  - □ Landscape Table on CD

- □ After Allowance Communication to TC
- □ Appeal Communication to Board of Appeals and Interferences
- ☑ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- □ Proprietary Information
- □ Status Letter
- ☑ Other Enclosure(s) (please Identify below):

Return Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Winstead Sechrest & Minick P.C.		
Signature			
Printed name	Robert A. Voigt, Jr.		
Date	09/22/2005	Reg. No.	47,159

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Toni Stanley		
Typed or printed name	Toni Stanley	Date	09/22/2005

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/17 (11-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 10/01/2004. Patent fees are subject to annual revision.

FEE TRANSMITTAL
For FY 2005

□ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($) 500.00

Complete if Known

Application Number	09/640,839
Filing Date	08/16/2000
First Named Inventor	Mark McClanahan
Examiner Name	Benjamin E. Lanier
Art Unit	2132
Attorney Docket No.	RPS920000052US1

METHOD OF PAYMENT (check all that apply)

□ Check □ Credit Card □ Money Order

☑ Deposit Account □ None

Deposit Account Number	50-0563
Deposit Account Name	IBM Corporation

The Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below

□ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17

☑ Credit any overpayments

to the above–identified deposit account.

□ Other (please identify):________

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING FEE

Fee Description	Fee ($)	Small Entity Fee ($)	Fee Paid($)
Utility Filing Fee	790	395	
Design Filing Fee	350	175	
Plant Filing Fee	550	275	
Reissue Filing Fee	790	395	
Provisional Filing Fee	160	80	

Subtotal (1) $________

FEE CALCULATION (continued)

2. EXTRA CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20	50	25
Each independent claim over 3	200	100
Multiple dependent claims	360	180
For Reissues, each claim over 20 and more than in the original patent	50	25
For Reissues, each independent claim more than in the original patent	200	100

Total Claims		Extra Claims		Fee ($)		Fee Paid ($)
____	- 20 or HP =	____	x	____	=	____

HP = highest number of total claims paid for, if greater than 20

Indep. Claims		Extra Claims		Fee ($)		Fee Paid ($)
____	- 3 or HP =	____	x	____	=	____

HP = highest number of independent claims paid for, if greater than 3

Multiple Dependent Claims	Fee ($)	Fee Paid ($)
	____	____

Subtotal (2) $________

3. OTHER FEES

Fee Description	Fee ($)	Small Entity Fee ($)	Fee Paid($)
1-month extension of time	120	60	
2-month extension of time	450	225	
3-month extension of time	1,020	510	
4-month extension of time	1,590	795	
5-month extension of time	2,160	1,080	
Information disclosure stmt. fee	180	180	
37 CFR 1.17(q) processing fee	50	50	
Non-English specification	130	130	
Notice of Appeal	500	250	
Filing a brief in support of appeal	500	250	500
Request for oral hearing	1,000	500	
Other:________			

Subtotal (3) $ 500

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 47,159	Telephone 512.370.2832
Name (Print/Type)	Robert A. Voigt, Jr.		Date 09/22/2005

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:
Mark G. McClanahan

Serial No.: 09/640,839

Filing Date: August 16, 2000

Title: SINGLE SIGN-ON TO AN
UNDERLYING OPERATING
SYSTEM APPLICATION

Before the Examiner:
Lanier, Benjamin E.

Group Art Unit: 2132

IBM Corporation
P.O. Box 12195
Dept. 9CCA, Bldg. 002-2
Research Triangle Park, NC 27709

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I. REAL PARTY IN INTEREST

The real party in interest is International Business Machines, Inc., which is the assignee of the entire right, title and interest in the above-identified patent application.

CERTIFICATION UNDER 37 C.F.R. §1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on September 22, 2005.

Toni Stanley
Signature

Toni Stanley
(Printed name of person certifying)

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant, Appellant's legal representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-81 are pending in the Application. Claims 1-81 stand rejected. Claims 1-81 are appealed.

IV. STATUS OF AMENDMENTS

Appellant has not submitted any amendments following receipt of the final rejection with a mailing date of July 1, 2005.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In one embodiment of the present invention, a method of bypassing an initial sign-on screen of an underlying operating system with a single sign-on capability may comprise the step of providing an application framework, where the application framework logs on a user with a first level of access in the underlying operating system. Specification, page 7, line 21- page 10, line 9; Figure 2, step 210. The method may further comprise generating an application framework sign-on screen. Specification, page 10, lines 10-11; Figure 2, step 220. The method may further comprise entering a logon input on the generated application framework sign-on screen. Specification, page 10, lines 11-12; Figure 2, step 230. The method may further comprise comparing the logon input with an application framework security database to determine level of access. Specification, page 10, lines 12-16; Figure 2, step 240.

In another embodiment of the present invention, a computer program product having a computer readable medium having computer program logic recorded thereon for bypassing an initial sign-on screen of an underlying operating system with a single sign capability may comprise programming operable for providing an application framework, where the application framework logs on a user with a first level of access in the underlying operating system. Specification, page 6, line 19 – page 7, line 16; Specification, page 7, line 21- page 10, line 9; Figure 1, elements 14, 20; Figure 2, step 210. The computer program product may further comprise programming operable for generating an application framework sign-on screen. Specification, page 6, line 19 – page 7, line 16; Specification, page 10, lines 10-11; Figure 1, elements 14, 20; Figure 2, step 220. The computer program product may further comprise programming operable for receiving a logon input entered on the generated application framework sign-on screen. Specification, page 6, line 19 – page 7, line 16; Specification, page 10, lines 11-12; Figure 1, elements 14, 20; Figure 2, step 230. The computer program product may further comprise programming operable for comparing the logon input with an application framework security database to determine level of access. Specification, page 6, line 19 – page 7, line 16; Specification, page 10, lines 12-16; Figure 1, elements 14, 20; Figure 2, step 240.

In another embodiment of the present invention, a data processing system may comprise a processor. Specification, page 6, line 19 – page 7, line 16; Figure 1, element 10. The data processing system may further comprise a memory unit operable for storing a computer program operable for bypassing an initial sign-on screen of an underlying operating system with a single sign capability. Specification, page 6, line 19 – page 7, line 16; Figure 1, elements 14, 20. The data processing system may further comprise an input mechanism. Specification, page 6, line 19 – page 7, line 16; Figure 1, elements 24, 26. The data processing system may further comprise an output mechanism. Specification, page 6, line 19 – page 7, line 16; Figure 1, element 38. The data processing system may further comprise a bus system coupling the processor to the memory unit, input mechanism, and output mechanism.

Specification, page 6, line 19 – page 7, line 16; Figure 1, element 12. The computer program is operable for performing the programming step of providing an application framework, where the application framework logs on a user with a first level of access in the underlying operating system. Specification, page 6, line 19 – page 7, line 16; Specification, page 7, line 21- page 10, line 9; Figure 1, elements 14, 20; Figure 2, step 210. The computer program may be further operable for performing the programming step of generating an application framework sign-on screen. Specification, page 6, line 19 – page 7, line 16; Specification, page 10, lines 10-11; Figure 1, elements 14, 20; Figure 2, step 220. The computer program may be further operable for performing the programming step of receiving a logon input entered on the generated application framework sign-on screen. Specification, page 6, line 19 – page 7, line 16; Specification, page 10, lines 11-12; Figure 1, elements 14, 20; Figure 2, step 230. The computer program may be further operable for performing the programming step of comparing the logon input with an application framework security database to determine level of access. Specification, page 6, line 19 – page 7, line 16; Specification, page 10, lines 12-16; Figure 1, elements 14, 20; Figure 2, step 240.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellant regards as the invention. Claims 1-8, 10-13, 15-20, 22, 23, 28-35, 37-40, 42-47, 49, 50, 55-62, 64-67, 69-74 and 76-77 stand rejected under 35 U.S.C. §102(b) as being anticipated by He (U.S. Patent No. 5,944,824).

VII. ARGUMENT

A. Claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 are not properly rejected under 35 U.S.C. §112, second paragraph.

The Examiner has rejected claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellant regards as the invention. Paper No. 10, page 6. In particular, the Examiner states:

> Claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75, 81 recite the limitation 'logging off said user with first level of access, wherein said underlying operating system logs on said user with said second level of access' which renders the claim indefinite because it is unclear which level of access the user possesses. Paper No. 10, page 6.

Appellant respectfully traverses the assertion that claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 are indefinite. Appellant respectfully contends that the scope of the claimed subject matter in claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75, 81 can be determined by one having ordinary skill in the art. Appellant respectfully directs the Board's attention to at least page 10, lines 18-30; page 12, lines 7-23 and page 14, lines 11-26 of the Specification as support for the above-cited claimed subject matter. Consequently, the scope of the above-cited claimed subject matter can be determined by one having ordinary skill in the art.

The Examiner has not provided any evidence that a person of ordinary skill in the art would not be able to determine the scope of the above-cited claimed subject matter. A rejection under 35 U.S.C. §112, second paragraph, is not appropriate, when the scope of the claimed subject matter can be determined by one having ordinary skill in the art. M.P.E.P. §706.03(d). As stated above, one having ordinary skill in the art can determine the scope of the claimed subject matter in claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81. Consequently, Appellant respectfully asserts that claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 are allowable under 35 U.S.C. §112, second paragraph.

Further, the purpose of the claim is not to explain technology or how it works. *S3 Inc. v. nVIDIA Corp.*, 59 U.S.P.Q.2d 1745, 1748 (Fed. Cir. 2001). The purpose is to state the legal boundaries of the patent grant. *Id.* As understood by the Appellant, the Examiner is rejecting claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 under 35 U.S.C. §112, second paragraph, for not explaining how it works. This is not an appropriate rationale for rejecting claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 under 35 U.S.C. §112, second paragraph. As stated above, the question that the Examiner must address in a rejection under 35 U.S.C. §112, second paragraph, is whether the scope of the claimed subject matter can be determined by one having ordinary skill in the art. M.P.E.P. §706.03(d). Since one having ordinary skill in the art can determine the scope of the claimed subject matter in claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81, claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 are allowable under 35 U.S.C. §112, second paragraph.

In response to Appellant's above argument, the Examiner states:

> The claims are requiring 'logging off said user with first level of access, wherein said underlying operating system logs on said user with said second level of access", which render the claims vague and indefinite because they appear to require two different users, one with a first level of access and one with a second level of access. The specification and the previous claims from which the above mentioned claims depend claim switching user level of access 'to' a different level, where this limitation requires switching 'users with' a level of access to a user with another level of access, which renders the claim vague and indefinite because the scope of the claim cannot be determined by the specification or the claims. Paper No. 10, page 5.

Appellant respectfully asserts that claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 do not recite multiple users. Neither is there a requirement specified in these claims or in the Specification for having two different users as intimated by the

Examiner. Neither do these claims recite the limitation of "users with" as suggested by the Examiner. The Examiner has not provided any evidence that a person of ordinary skill in the art would not be able to determine the scope of the above-cited claimed subject matter. Consequently, Appellant respectfully asserts that claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75 and 81 are allowable under 35 U.S.C. §112, second paragraph.

B. Claims 1-8, 10-13, 15-20, 22, 23, 28-35, 37-40, 42-47, 49, 50, 55-62, 64-67, 69-74 and 76-77 are not properly rejected under 35 U.S.C. §102(b) as being anticipated by He.

The Examiner has rejected claims 1-8, 10-13, 15-20, 22, 23, 28-35, 37-40, 42-47, 49, 50, 55-62, 64-67, 69-74 and 76-77 under 35 U.S.C. §102(e) as being anticipated by He. Paper No. 10, page 6. Appellant respectfully traverses these rejections for at least the reasons stated below and respectfully requests that the Examiner reconsider and withdraw these rejections.

For a claim to be anticipated under 35 U.S.C. §102, each and every claim limitation must be found within the cited prior art reference and arranged as required by the claim. M.P.E.P. §2131.

1. Claims 1, 28 and 55 are not anticipated by He.

Appellant respectfully asserts that He does not disclose "providing an application framework, wherein said application framework logs on a user with a first level of access in said underlying operating system" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites column 2, line 25 – 32 of He as disclosing the above-cited claim limitation. Paper No. 10, page 7. Appellant respectfully traverses and asserts that He instead discloses a single sign-on that allows a user to log-on only once at a user station and a security server that will, in turn, automatically log the user on to all the network elements that the user is authorized to access. There is no language in the cited passage that discloses an application framework that logs a user in the underlying operation system. Neither is there any language in the cited passage that discloses an application framework that logs a user with a first level of access in the underlying operation system. Thus, He does not disclose all of the limitations of claims 1, 28 and 55, and thus He does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

In response to the above argument, the Examiner, as understood by the Appellant, asserts that the above-cited claim limitation is necessarily disclosed since He's SSO system permits a single sign-on of users to network elements. Paper No. 10, page 2. However, the Examiner has provided no evidence that the teaching of permitting a single sign-on of users to network elements necessarily teaches providing an application framework, where the application framework logs on a user with a first level of access in the underlying operating system. The Examiner simply makes assertions without providing any basis in fact and/or technical reasoning to support such a conclusion. The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that the teaching of permitting a single sign-on of users to network elements necessarily teaches providing an application framework, where the application framework logs on a user with a first level of access in the underlying operating system. *See Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). Since the Examiner is simply relying upon his own subjective opinion without providing any objective evidence, the Examiner has not established a *prima facie* case of anticipation in rejecting claims 1, 28 and 55. M.P.E.P. §2131.

Appellant further asserts that He does not disclose "generating an application framework sign-on screen" as recited in claim 1 and similarly in claims 28 and 55.

The Examiner cites column 2, line 25 – 32 of He as disclosing the above-cited claim limitation. Paper No. 10, page 7. Appellant respectfully traverses. As stated above, He instead discloses a single sign-on that allows a user to log-on only once at a user station and a security server that will, in turn, automatically log the user on to all the network elements that the user is authorized to access. There is no language in the cited passage that discloses an application framework. The Specification defines an application framework (page 7, lines 27-28) as controlling what applications are accessible to the particular user. Neither is there any language in the cited passage that discloses an application framework sign-on screen. The cited passage does disclose the term "single sign-on" but there is no language in the cited passage that discloses a sign-on screen. Thus, He does not disclose all of the limitations of claims 1, 28 and 55, and thus He does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

In response to the above argument, the Examiner, as understood by the Appellant, asserts that the above-cited claim limitation is necessarily disclosed since He's SSO system permits a single sign-on of users to network elements. Paper No. 10, page 2. However, the Examiner has provided no evidence that the teaching of permitting a single sign-on of users to network elements necessarily teaches generating an application framework sign-on screen. The Examiner simply makes assertions without providing any basis in fact and/or technical reasoning to support such a conclusion. The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that the teaching of permitting a single sign-on of users to network elements necessarily teaches generating an application framework sign-on screen. *See Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). Since the Examiner is simply relying upon his own subjective opinion without providing any objective evidence, the Examiner has not established a *prima facie* case of anticipation in rejecting claims 1, 28 and 55. M.P.E.P. §2131.

Further, in response to the above argument, the Examiner cites Figure 1 as disclosing an application framework sign-on screen. The Examiner has not specifically identified any element in Figure 1 as allegedly disclosing an application framework sign-on screen. Appellant was unable to identify an application framework sign-on screen in Figure 1. Thus, He does not disclose all of the limitations of claims 1, 28 and 55, and thus He does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Appellant further asserts that He does not disclose "entering a logon input on said generated application framework sign-on screen" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites column 2, line 25 – 32 of He as disclosing the above-cited claim limitation. Paper No. 10, page 7. Appellant respectfully traverses. As stated above, He instead discloses a single sign-on that allows a user to log-on only once at a user station and a security server that will, in turn, automatically log the user on to all the network elements that the user is authorized to access. As stated above, there is no language in the cited passage that discloses an application framework. Neither is there any language in the cited passage that discloses an application framework sign-on screen. Neither is there any language in the cited passage that discloses entering a login input on the generated application framework sign-on screen. The cited passage does disclose the term "single sign-on" but there is no language in the cited passage that discloses a sign-on screen or entering a login input on the sign-on screen. Thus, He does not disclose all of the limitations of claims 1, 28 and 55, and thus He does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Appellant further asserts that He does not disclose "comparing said logon input with an application framework security database to determine level of access" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites column 5, lines 8-15 of He as disclosing the above-cited claim limitation. Paper No. 10, page 7. Appellant respectfully traverses. He instead discloses that a request is sent to a user station requesting a user identifier and a password. Column 5, lines 7-9. He further discloses that the user information will be checked against the information in the user profile of a central security database at a security server. Column 5, lines 9-11. He further discloses that a network establishes mutual trust between an authenticated user and a specific mutual trust between an authenticated user and a specific NE the user requests to access. Column 5, lines 11-13. He further discloses that the network authentication assures the user that the correct NE is accessed. Column 5, lines 13-15. However, there is no language in the cited passage that discloses comparing login input with a database <u>to determine the level of access</u>. Instead, He simply discloses ensuring that the user is authenticated to access the correct network element. Thus, He does not disclose all of the limitations of claims 1, 28 and 55, and thus He does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

2. <u>Claims 2-8, 10-13, 15-20, 22, 23, 29-35, 37-40, 42-47, 49, 50, 56-62, 64-67, 69-74 and 76-77 are not anticipated by He for at least the reasons that claims 1, 28 and 55 are not anticipated by He.</u>

Claims 2-8, 10-13, 15-20, 22 and 23 depend from claim 1 and hence are not anticipated by He for at least the reasons that claim 1 is not anticipated by He as discussed above in Section B.1. Claims 29-35, 37-40, 42-47, 49 and 50 depend from claim 28 and hence are not anticipated by He for at least the reasons that claim 28 is not anticipated by He as discussed above in Section B.1. Claims 56-62, 64-67, 69-74 and 76-77 depend from claim 55 and hence are not anticipated by He for at least the reasons that claim 55 is not anticipated by He as discussed above in Section B.1

3. <u>Claims 2, 29 and 56 are not anticipated by He.</u>

Appellant respectfully asserts that He does not disclose "selecting an indication of said first level of access" as recited in claim 2 and similarly in claims 29 and 56. The Examiner cites column 5, lines 8-15 of He as disclosing the above-cited claim limitation. Paper No. 10, page 7. Appellant respectfully traverses. As stated above, He instead discloses that a request is sent to a user station requesting a user identifier and a password. Column 5, lines 7-9. He further discloses that the user information will be checked against the information in the user profile of a central security database at a security server. Column 5, lines 9-11. He further discloses that a network establishes mutual trust between an authenticated user and a specific mutual trust between an authenticated user and a specific NE the user requests to access. Column 5, lines 11-13. He further discloses that the network authentication assures the user that the correct NE is accessed. Column 5, lines 13-15. However, there is no language in the cited passage that discloses <u>selecting an indication</u> of a <u>first level of access</u>. Instead, He discloses assuring the user that the correct network element is accessed. Thus, He does not disclose all of the limitations of claims 2, 29 and 56, and thus He does not anticipate claims 2, 29 and 56. M.P.E.P. §2131.

In response to the above argument, the Examiner states:

> Applicant's argument that He does not disclose selecting an indication of said first level of access is not persuasive because the selection of the authorized NEs for the specific users are an indication of the user level of access. Paper No. 10, page 3.

Appellant respectfully traverses the assertion that by teaching the accessing of a network element that He necessarily discloses selecting an indication of a first level of access. The Examiner has not identified any passage in He as disclosing an indication of a level of access. The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that the teaching of accessing a network element necessarily teaches selecting an indication of a first level of access. *See Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). Since the Examiner is simply relying upon his own subjective opinion without providing any objective evidence, the Examiner has not established a *prima facie* case of anticipation in rejecting claims 2, 29 and 56. M.P.E.P. §2131.

4. Claims 3, 30 and 57 are not anticipated by He.

Appellant respectfully asserts that He does not disclose "wherein said user is logged onto said underlying operating system and an application environment with said first level of access thereby bypassing said initial sign-on screen of said underlying operating system with said single sign-on" as recited in claim 3 and similarly in claims 30 and 57. The Examiner cites column 5, lines 8-15 of He as disclosing the above-cited claim limitation. Paper No. 10, page 7. Appellant respectfully traverses. As stated above, He instead discloses assuring the user that the correct network element is accessed. There is no language in the cited passage that discloses logging onto an underlying operating system and an application environment. Neither is there any language in the cited passage that discloses logging onto an underlying operating system and an application environment with a first level of access. Neither is there any language in the cited passage that discloses logging onto an underlying operating system and an application environment with a first level of access thereby bypassing an initial sign-on screen of the underlying operating system with the single sign-on. Thus, He does not disclose all of the limitations of claims 3, 30 and 57, and thus He does not anticipate claims 3, 30 and 57. M.P.E.P.

§2131.

5. Claims 4, 10, 16, 24, 31, 37, 43, 51, 58, 64, 70 and 78 are not anticipated by He.

Appellant respectfully asserts that He does not disclose "wherein if said logon input is not entitled to a second level of access according to said application framework security database, then said user is logged onto an application environment and said underlying operating system as said first level of access" as recited in claim 4 and similarly in claims 31 and 58. Appellant further asserts that He does not disclose "wherein if said logon input is not entitled to a second level of access according to said application framework security database, then an indication of said second level of access will not be generated to said user, wherein said user is restricted to said first level of access" as recited in claim 10 and similarly in claims 37 and 64. Appellant further asserts that He does not disclose "wherein if said logon input is not entitled to said second level of access according to said application framework security database, then said user is restricted to said first level of access" as recited in claim 16 and similarly in claims 43 and 70. Appellant further asserts that He does not disclose "wherein if said underlying operating system security database does not verify said user with access to said second level of access, then said user is restricted to said first level of access" as recited in claim 24 and similarly in claims 51 and 78. The Examiner cites column 5, lines 41-58 and column 8, lines 40-65 of He as disclosing the above-cited claim limitations. Paper No. 10, page 8. Appellant respectfully traverses.

He instead discloses a user privilege determines the set of network elements a user can access. Column 5, lines 41-42. He further discloses that the network element password recovery for a user requires the presence and authority of a "super user" to a network element. Column 8, lines 40-41.

None of this language discloses logging a user onto an application environment and an underlying operating system as a first level of access. Neither does this language disclose logging a user onto an application environment and an underlying operating system as a first level of access if the logon input is not entitled to a second level of access according to an application framework security database. Neither does this language disclose not generating an indication of a second level of access. Neither does this language disclose not generating an indication of a second level of access if the logon input is not entitled to a second level of access according to an application framework security database. Neither does this language disclose that the user is restricted to a first level of access. Neither does this language disclose that the user is restricted to a first level of access if the login input is not entitled to a second level of access according to an application framework security database. Neither does this language discloses that if the underlying operating system security database does not verify the user with access to the second level of access, then the user is restricted to the first level of access. Thus, He does not disclose all of the limitations of claims 4, 10, 16, 24, 31, 37, 43, 51, 58, 64, 70 and 78, and thus He does not anticipate claims 44, 10, 16, 24, 31, 37, 43, 51, 58, 64, 70 and 78. M.P.E.P. §2131.

In response to the above argument, the Examiner states:

> Applicant's argument that He does not disclose if said logon input is not entitled to a second level of access according to said application framework security database, then said user is logged onto an application environment and said underlying operating system as said first level of access is not persuasive because He discloses that the user privilege level determines the access rights that the user has and what network elements the user can access (Col. 5, lines 41-45). Unless the user is granted additional access rights (Col. 5, lines 45-48 & Col. 8, lines 40-65), the user can only access the network elements designated to that user as being authorized for their use, and attempted accesses of unauthorized network elements will be rejected and logged (Col. 5, lines 49-58), which further meets the limitation of if said logon input is not entitled to a second level of access of access according to said

> application framework security database, then an indication of said second level of access will not be generated to said user, wherein said user is restricted to said first level of access. Paper No. 10, pages 3-4.

Appellant respectfully traverses the Examiner's assertion that He discloses the above-cited claim limitations. The Examiner has not provided any basis in fact and/or technical reasoning to support the assertion that the teaching of a user privilege determines the set of NEs a user can access (column 5, lines 41-42 of He) as well as the teaching of logging all user access attempts necessarily discloses "wherein if the logon input is not entitled to a second level of access according to the application framework security database, then the user is logged onto an application environment and the underlying operating system as the first level of access." The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that the teaching of a user privilege determines the set of NEs a user can access (column 5, lines 41-42 of He) as well as the teaching of logging all user access attempts necessarily discloses "wherein if the logon input is not entitled to a second level of access according to the application framework security database, then the user is logged onto an application environment and the underlying operating system as the first level of access." *See Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). Further, the Examiner must provide a basis in fact and/or technical reasoning to support the assertion that the teaching of a user privilege determines the set of NEs a user can access (column 5, lines 41-42 of He) as well as the teaching of logging all user access attempts necessarily discloses the other above-recited claim limitations. *Id.* Since the Examiner is simply relying upon his own subjective opinion without providing any objective evidence, the Examiner has not established a *prima facie* case of anticipation in rejecting claims 4, 10, 16, 24, 31, 37, 43, 51, 58, 64, 70 and 78. M.P.E.P. §2131.

6. Claims 6, 17, 19, 22, 25, 34, 44, 46, 49, 52, 61, 71, 73, 76 and 79 are not anticipated by He.

Appellant respectfully asserts that He does not disclose "executing a switch user program to switch said user to said second level of access" as recited in claim 6 and similarly in claims 34 and 61. Appellant further asserts that He does not disclose "executing a switch user program to switch said user to said second level of access" as recited in claim 17 and similarly in claims 44 and 71. Appellant further asserts that He does not disclose "comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access" as recited in claim 19 and similarly in claims 46 and 73. Appellant further asserts that He does not disclose "comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database does not verify said user with access to said second level of access, then the method further comprises the step of: requesting from said user a logon identification; and comparing said logon identification with said underlying operating system security database" as recited in claim 22 and similarly in claims 49 and 76. Appellant further asserts that He does not disclose "wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access" as recited in claim 25 and similarly in claims 52 and 79. The Examiner cites column 8, lines 51-54 as disclosing the above-cited claim limitations. Paper No. 10, page 8. Appellant respectfully traverses.

He instead discloses that the security control on the different types of super users is the same as that for the ordinary users except that these users are granted more privileges to perform administrative functions in a network element. Column 8, lines 49-52.

None of this language discloses executing a program to switch user to a second level of access. Neither does this language disclose comparing logon input with an underlying operating system security database. Neither does this language disclose that if the underlying operating system security database verifies the user with access to the second level of access, then the switch user program switches the user to the second level of access. Neither does this language disclose that if the underlying operating system security database does not verify the user with access to the second level of access, then a logon identification is requested from the user; and the logon identification is compared with the underlying operating system security database. Neither does this language disclose that if the underlying operating system security database verifies the user with access to the second level of access, then the switch user program switches the user to the second level of access. Thus, He does not disclose all of the limitations of claims 6, 17, 19, 22, 25, 34, 44, 46, 49, 52, 61, 71, 73, 76 and 79, and thus He does not anticipate claims 6, 17, 19, 22, 25, 34, 44, 46, 49, 52, 61, 71, 73, 76 and 79. M.P.E.P. §2131.

In response to the above argument, the Examiner maintains the assertion that the teaching of granting more privileges to perform administrative functions in a network element (column 8, lines 51-54 of He) teaches the above-cited claim limitations. Paper No. 10, page 4. Appellant respectfully traverses. The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that the teaching of granting more privileges to perform administrative functions in a network element (column 8, lines 51-54 of He) teaches the above-cited claim limitations. *See Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). Since the Examiner is simply relying upon his own subjective opinion without providing any objective evidence, the Examiner has not established a *prima facie* case of anticipation in rejecting claims 6, 17, 19, 22, 25, 34, 44, 46, 49, 52, 61, 71, 73, 76 and 79. M.P.E.P. §2131.

7. Claims 8, 13, 20, 26, 35, 40, 47, 53, 62, 67, 74 and 80 are not anticipated by He.

Appellant respectfully asserts that He does not disclose "wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry" as recited in claim 8 and similarly in claims 13, 35, 40, 62 and 67. Appellant further asserts that He does not disclose "wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry" as recited in claim 20 and similarly in claims 47 and 74. Appellant further asserts that He does not disclose "wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry" as recited in claim 26 and similarly in claims 53 and 80. The Examiner cites column 5, lines 41-48 and column 15, lines 52-53 of He as disclosing the above-cited claim limitations. Paper No. 10, pages 8-9. Appellant respectfully traverses.

He instead discloses that for the user privilege control module, a user privilege determines the set of network elements a user can access. Column 5, lines 41-42. He further discloses that all user account and network element data are maintained in a database, called DCE registry, at the SS node. Column 15, lines 52-54.

There is no language in the cited passages that discloses switching a user to a second level of access. Neither is there any language in the cited passages that discloses switching a user to the second level of access by modifying an underlying operating system's registry. Thus, He does not disclose all of the limitations of claims 8, 13, 20, 26, 35, 40, 47, 53, 62, 67, 74 and 80, and thus He does not anticipate claims 8, 13, 20, 26, 35, 40, 47, 53, 62, 67, 74 and 80. M.P.E.P. §2131.

In response to the above argument, the Examiner states:

Applicant's argument...is not persuasive because He discloses that the

> user records, stored in registry (Col .15, lines 52-53) are modified to give the user more access rights (Col. 5, lines 41-48). Paper No. 10, page 4.

Appellant respectfully traverses and asserts that He discloses that a user privilege determines the set of network elements a user can access. Column 5, lines 41-42. He further discloses that the user privilege control must reflect the policy of 'need-to-know' that can be established based on the responsibility of the position of the user inside a company. Column 5, lines 42-45. He further discloses that change of user privilege can be easily made to reflect the present responsibility of the user, which in turn determines the access right of the user to the network elements. Column 5, lines 45-48. He further discloses that all user account and network element data are maintained in a database, called DCE registry, at the SS node. Column 15, lines 52-54. There is no language in column 5, lines 41-48 and column 15, lines 52-54 of He that supports the Examiner's assertion that He discloses modifying records in a registry to give the user more access rights. Instead, He discloses that by changing the user privilege that the access right of the user to the network elements may be changed. The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that the teaching of changing the user privilege may change the access right of the user to the network elements which necessarily infers the teaching of the above-cited claim limitations. *See Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). Since the Examiner is simply relying upon his own subjective opinion without providing any objective evidence, the Examiner has not established a *prima facie* case of anticipation in rejecting claims 8, 13, 20, 26, 35, 40, 47, 53, 62, 67, 74 and 80. M.P.E.P. §2131.

8. Claims 11, 12, 15, 38, 39, 42, 65, 66 and 69 are not anticipated by He.

Appellant respectfully asserts that He does not disclose "wherein if said logon input is entitled to a second level of access according to said application framework security database, then the method further comprises the step of: generating an indication of said second level of access" as recited in claim 11 and similarly in claims 38 and 65. Appellant further asserts that He does not disclose "executing a switch user program to switch level of access to said second level of access by selecting said indication of said second level of access" as recited in claim 12 and similarly in claims 39 and 66. Appellant further asserts that He does not disclose "selecting an indication of a second level of access" as recited in claim 15 and similarly in claims 42 and 69. The Examiner cites column 10, line 58 – column 11, line 10 of He as disclosing the above-cited claim limitations. Paper No. 10, page 9. Appellant respectfully traverses.

He instead discloses that the SSO Indication Digit specifies whether SSO is allowed for a user. Column 10, lines 58-59. He further discloses that if the indication is that the user is not allowed, the list following it shall be ignored in its entirety. Column 10, lines 59-61. He further discloses that if the user is allowed, then the existence of an item for the specified network element in the list determines whether the user is allowed the SSO capability to that particular network element. Column 10, lines 61-63.

There is no language in the cited passage that discloses that if the logon input is entitled to a second level of access according to an application framework security database, then an indication of a second level of access is generated. Neither is there any language in the cited passage that discloses executing a switch user program to switch a level of access to a second level of access by selecting the indication of the second level of access. Neither is there any language in the cited passage that discloses selecting an indication of a second level of access. Thus, He does not disclose all of the limitations of claims 11, 12, 15, 38, 39, 42, 65, 66 and 69, and thus He does not anticipate claims 11, 12, 15, 38, 39, 42, 65, 66 and 69. M.P.E.P. §2131.

In response to the above argument, the Examiner states:

> Applicant's argument...is not persuasive because He discloses that the SSO contains an indication digit for regular users and for super users (Col. 10, line 58 – Col. 11, line 10). Paper No. 10, page 5.

Appellant respectfully traverses the assertion that He discloses any of the above-cited claim limitations. He instead discloses that the SSO indication digit specifies whether SSO is allowed for this user. Column 10, lines 58-59. He further discloses that if the indication is that the user is not allowed, the list following it shall be ignored in its entirety. Column 10, lines 59-61. He further discloses that if the user is allowed, then the existence of an item for the specified network element in the list determines whether the user is allowed the SSO capability to that particular network element. Column 10, lines 61-63. He further discloses that this enhancement only affects the security server node in the security database. Column 10, lines 63-65. Hence, He discloses an indication digit that specifies whether the SSO is allowed for a particular user.

There is no language in the cited passage that discloses that <u>if the logon input is entitled to a second level of access</u> according to an application framework security database, then <u>an indication of a second level of access is generated</u>. Neither is there any language in the cited passage that discloses <u>executing a switch user program to switch a level of access to a second level of access by selecting the indication of the second level of access</u>. Neither is there any language in the cited passage that discloses <u>selecting an indication of a second level of access</u>. Thus, He does not disclose all of the limitations of claims 11, 12, 15, 38, 39, 42, 65, 66 and 69, and thus He does not anticipate claims 11, 12, 15, 38, 39, 42, 65, 66 and 69. M.P.E.P. §2131.

9. <u>Claims 18, 45 and 72 are not anticipated by He.</u>

Appellant respectfully asserts that He does not disclose "transferring said logon input to said underlying operating system for verification" as recited in claim

18 and similarly in claims 45 and 72. The Examiner cites column 5, lines 8-15 of He as disclosing the above-cited claim limitation. Paper No. 10, page 7. Appellant respectfully traverses and asserts that He instead discloses that a request is sent to a user station requesting a user identifier and a password. Column 5, lines 7-9. He further discloses that the user information will be checked against the information in the user profile of a central security database at a security server. Column 5, lines 9-11. He further discloses that a network establishes mutual trust between an authenticated user and a specific mutual trust between an authenticated user and a specific NE the user requests to access. Column 5, lines 11-13. He further discloses that the network authentication assures the user that the correct NE is accessed. Column 5, lines 13-15. However, there is no language in the cited passage that discloses transferring a logon input to an underlying operating system for verification. Thus, He does not disclose claims 18, 45 and 72, and thus He does not anticipate claims 18, 45 and 72. M.P.E.P. §2131.

In response to the above argument, the Examiner states:

> Applicant's argument...He discloses that the user attempts to log-on the information entered by the user is checked against the information in the user profile of the central security database at the security server and assures that the user accesses the correct network elements based on the user privilege (Col. 5, lines 8-15). Paper No. 10, page 5.

Appellant respectfully traverses the assertion that He discloses the above-cited claim limitation. He instead discloses that the user information will be checked against the information in the user profile of the central security database at the security server. Column 5, lines 9-11. He further discloses that the network establishes mutual trust between an authenticated user and a specific network element the user requests to access. Column 5, lines 11-13. He further discloses that therefore, network authentication 50 also assures the user that the correct network element is accessed. Column 5, lines 13-15. Thus, He discloses that the user information will be checked against the information in the user profile of the central security database at the security server. He further discloses that network authentication 50 also assures the user that the correct network element is accessed.

However, there is no language in the cited passage that discloses transferring logon input to an underlying operating system. Neither is there any language in the cited passage that discloses transferring logon input to an underlying operating system for verification. Instead, He simply discloses that the user information will be checked against the information in the user profile of the central security database at the security server. Thus, He does not disclose claims 18, 45 and 72, and thus He does not anticipate claims 18, 45 and 72. M.P.E.P. §2131.

VIII. CONCLUSION

For the reasons noted above, the rejections of claims 1-81 are in error. Appellant respectfully requests reversal of the rejections and allowance of claims 1-81.

Respectfully submitted,
WINSTEAD SECHREST & MINICK P.C.
Attorneys for Appellant

By:____________________
Robert A. Voigt, Jr.
Reg. No. 47,159
Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2832

CLAIMS APPENDIX

1. A method of bypassing an initial sign-on screen of an underlying operating system with a single sign-on capability comprising the steps of:

providing an application framework, wherein said application framework logs on a user with a first level of access in said underlying operating system;

generating an application framework sign-on screen;

entering a logon input on said generated application framework sign-on screen; and

comparing said logon input with an application framework security database to determine level of access.

2. The method as recited in claim 1 further comprising the step of:

selecting an indication of said first level of access.

3. The method as recited in claim 1, wherein said user is logged onto said underlying operating system and an application environment with said first level of access thereby bypassing said initial sign-on screen of said underlying operating system with said single sign-on.

4. The method as recited in claim 1, wherein if said logon input is not entitled to a second level of access according to said application framework security database, then said user is logged onto an application environment and said underlying operating system as said first level of access.

5. The method as recited in claim 1, wherein said logon input comprises a user identification and a user password.

6. The method as recited in claim 1, wherein if said logon input is entitled to a second level of access according to said application framework security database, then the method further comprises the step of:

executing a switch user program to switch said user to said second level of access.

7. The method as recited in claim 1, wherein said application framework security database stores system operator information, wherein said application framework security database defines at least one of the following: users, passwords, groups of users and application specific authorization.

8. The method as recited in claim 7, wherein a switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

9. The method as recited in claim 8, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

10. The method as recited in claim 2, wherein if said logon input is not entitled to a second level of access according to said application framework security database, then an indication of said second level of access will not be generated to said user, wherein said user is restricted to said first level of access.

11. The method as recited in claim 2, wherein if said logon input is entitled to a second level of access according to said application framework security database, then the method further comprises the step of:

generating an indication of said second level of access.

12. The method as recited in claim 11 further comprising the step of:

executing a switch user program to switch level of access to said second level of access by selecting said indication of said second level of access.

13. The method as recited in claim 12, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

14. The method as recited in claim 13, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

15. The method as recited in claim 1 further comprising the step of:

selecting an indication of a second level of access.

16. The method as recited in claim 15, wherein if said logon input is not entitled to said second level of access according to said application framework security database, then said user is restricted to said first level of access.

17. The method as recited in claim 15, wherein if said logon input is entitled to said second level of access according to said application framework security database, then the method further comprises the step of:

executing a switch user program to switch said user to said second level of access.

18. The method as recited in claim 17 further comprising the step of:

transferring said logon input to said underlying operating system for verification.

19. The method as recited in claim 18 further comprising the step of:

comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access.

20. The method as recited in claim 19, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

21. The method as recited in claim 20, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

22. The method as recited in claim 18 further comprising the step of:

comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database does not verify said user with access to said second level of access, then the method further comprises the step of:

requesting from said user a logon identification; and

comparing said logon identification with said underlying operating system security database.

23. The method as recited in claim 22, wherein said logon identification comprises a user identification and a user password.

24. The method as recited in claim 22, wherein if said underlying operating system security database does not verify said user with access to said second level of access, then said user is restricted to said first level of access.

25. The method as recited in claim 22, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access.

26. The method as recited in claim 25, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

27. The method as recited in claim 26, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

28. A computer program product having a computer readable medium having computer program logic recorded thereon for bypassing an initial sign-on screen of an underlying operating system with a single sign capability, comprising:

programming operable for providing an application framework, wherein said application framework logs on a user with a first level of access in said underlying operating system;

programming operable for generating an application framework sign-on screen;

programming operable for receiving a logon input entered on said generated application framework sign-on screen; and

programming operable for comparing said logon input with an application framework security database to determine level of access.

29. The computer program product as recited in claim 28 further comprises:

programming operable for selecting an indication of said first level of access.

30. The computer program product as recited in claim 28, wherein said user is logged onto said underlying operating system and an application environment with said first level of access thereby bypassing said initial sign-on screen of said underlying operating system with said single sign-on.

31. The computer program product as recited in claim 28, wherein if said logon input is not entitled to a second level of access according to said application framework security database, then said user is restricted to said first level of access.

32. The computer program product as recited in claim 28, wherein said logon input comprises a user identification and a user password.

33. The computer program product as recited in claim 28, wherein said application framework security database stores system operator information, wherein said application framework security database defines at least one of the following: users, passwords, groups of users and application specific authorization.

34. The computer program product as recited in claim 28, wherein if said logon input is entitled to a second level of access according to said application framework security database, then the computer program product further comprises:

programming operable for executing a switch user program to switch said user to said second level of access.

35. The computer program product as recited in claim 34, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

36. The computer program product as recited in claim 35, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

37. The computer program product as recited in claim 29, wherein if said logon input is not entitled to a second level of access according to said application framework security database, then an indication of said second level of access will not be generated to said user, wherein said user is restricted to said first level of access.

38. The computer program product as recited in claim 29, wherein if said logon input is entitled to a second level of access according to said application framework security database, then the computer program product further comprises:

programming operable for generating an indication of said second level of access.

39. The computer program product as recited in claim 38 further comprises:

programming operable for executing a switch user program to switch level of access to said second level of access by selecting said indication of said second level of access.

40. The computer program product as recited in claim 39, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

41. The computer program product as recited in claim 40, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

42. The computer program product as recited in claim 28 further comprises:

programming operable for selecting an indication of a second level of access.

43. The computer program product as recited in claim 42, wherein if said logon input is not entitled to said second level of access according to said application framework security database, then said user is restricted to said first level of access.

44. The computer program product as recited in claim 42, wherein if said logon input is entitled to said second level of access according to said application framework security database, then the computer program product further comprises:

programming operable for executing a switch user program to switch said user to said second level of access.

45. The computer program product as recited in claim 44 further comprises:

programming operable for transferring said logon input to said underlying operating system for verification.

46. The computer program product as recited in claim 45 further comprises:

programming operable for comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access.

47. The computer program product as recited in claim 46, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

48. The computer program product as recited in claim 47, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

49. The computer program product as recited in claim 45 further comprises:

programming operable for comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database does not verify said user with access to said second level of access, then the computer program product further comprises:

programming operable for requesting from said user a logon identification; and

programming operable for comparing said logon identification with said underlying operating system security database.

50. The computer program product as recited in claim 49, wherein said logon identification comprises a user identification and a user password.

51. The computer program product as recited in claim 49, wherein if said underlying operating system security database does not verify said user with access to said second level of access, then said user is restricted to said first level of access.

52. The computer program product as recited in claim 49, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access.

53. The computer program product as recited in claim 52, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

54. The computer program product as recited in claim 53, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

55. A data processing system, comprising:

a processor;

a memory unit operable for storing a computer program operable for bypassing an initial sign-on screen of an underlying operating system with a single sign capability;

an input mechanism;

an output mechanism; and

a bus system coupling the processor to the memory unit, input mechanism, and output mechanism, wherein the computer program is operable for performing the following programming steps:

providing an application framework, wherein said application framework logs on a user with a first level of access in said underlying operating system;

generating an application framework sign-on screen;

receiving a logon input entered on said generated application framework sign-on screen; and

comparing said logon input with an application framework security database to determine level of access.

56. The data processing system as recited in claim 55, wherein the computer program is further operable to perform the programming step:

selecting an indication of said first level of access.

57. The data processing system as recited in claim 55, wherein said user is logged onto said underlying operating system and an application environment with said first level of access thereby bypassing said initial sign-on screen of said underlying operating system with said single sign-on.

58. The data processing system as recited in claim 55, wherein if said logon input is not entitled to a second level of access according to said application framework security database, then said user is logged onto an application environment and said underlying operating system as said first level of access.

59. The data processing system as recited in claim 55, wherein said logon input comprises a user identification and a user password.

60. The data processing system as recited in claim 55, wherein said application framework security database stores system operator information, wherein said application framework security database defines at least one of the following: users, passwords, groups of users and application specific authorization.

61. The data processing system as recited in claim 55, wherein if said logon input is entitled to a second level of access according to said application framework security database, then the computer program is further operable to perform the programming step:

executing a switch user program to switch said user to said second level of access.

62. The data processing system as recited in claim 61, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

63. The data processing system as recited in claim 62, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

64. The data processing system as recited in claim 56, wherein if said logon input is not entitled to a second level of access according to said application framework security database, then an indication of said second level of access will not be generated to said user, wherein said user is restricted to said first level of access.

65. The data processing system as recited in claim 56, wherein if said logon input is entitled to a second level of access according to said application framework security database, then the computer program is further operable to perform the programming step:

generating an indication of said second level of access.

66. The data processing system as recited in claim 65, wherein the computer program is further operable to perform the programming step:

executing a switch user program to switch level of access to said second level of access by selecting said indication of said second level of access.

67. The data processing system as recited in claim 65, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

68. The data processing system as recited in claim 67, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

69. The data processing system as recited in claim 55, wherein the computer program is further operable to perform the programming step:

selecting an indication of a second level of access.

70. The data processing system as recited in claim 69, wherein if said logon input is not entitled to said second level of access according to said application framework security database, then said user is restricted to said first level of access.

71. The data processing system as recited in claim 69, wherein if said logon input is entitled to said second level of access according to said application framework security database, then the computer program is further operable to perform the programming step:

executing a switch user program to switch said user to said second level of access.

72. The data processing system as recited in claim 71, wherein the computer program is further operable to perform the programming step:

transferring said logon input to said underlying operating system for verification.

73. The data processing system as recited in claim 72, wherein the computer program is further operable to perform the programming step:

comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access.

74. The data processing system as recited in claim 73, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

75. The data processing system as recited in claim 74, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

76. The data processing system as recited in claim 72, wherein the computer program is further operable to perform the programming step:

comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database does not verify said user with access to said second level of access, then the computer program is further operable to perform the programming steps:

requesting from said user a logon identification; and

comparing said logon identification with said underlying operating system security database.

77. The data processing system as recited in claim 76, wherein said logon identification comprises a user identification and a user password.

78. The data processing system as recited in claim 76, wherein if said underlying operating system security database does not verify said user with access to said second level of access, then said user is restricted to said first level of access.

79. The data processing system as recited in claim 76, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access.

80. The data processing system as recited in claim 79, wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

81. The data processing system as recited in claim 80, wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access.

EVIDENCE APPENDIX

No evidence was submitted pursuant to §§1.130, 1.131, or 1.132 of 37 C.F.R. or of any other evidence entered by the Examiner and relied upon by Appellant in the Appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings to the current proceeding.